ABSTRACT

A method and system for securing a data product for mass distribution. An authorization server may encrypt a portion of a data product. Further, the authorization server may assemble an authorization key that includes information indicative of an entity authorized to store the data product, and the authorization server may encrypt the authorization key. To encrypt the authorization key, the authorization server may apply a symmetric encryption algorithm based on a cryptographic key that is derived as a function of an identification code associated with the authorized entity. The encrypted portion of the data product, the encrypted authentication key, and the remainder of the data product may then be stored on the authorized entity, which may be provided to a machine authorized to access the data product. The machine is preferably programmed to derive the second decryption key, use it to decrypt the authentication key, and then use the authentication key to validate use of the data product. Advantageously, if the data product is copied to an unauthorized entity and that entity is then provided to the machine, the machine may be unable to obtain the necessary identification code and may therefore be unable to derive the cryptographic key, to decrypt the authentication key, or to validate access to the data product.